



Cisco Cloud Services Platform 2100 Quick Start Guide, Release 2.2.0

First Published: 2017-03-15

Last Modified: 2017-08-03

Setting Up Your Cisco CSP 2100 and Configuring Services

Summary Steps

Setting up your Cisco Cloud Services Platform 2100 (Cisco CSP 2100) and creating services consists of the following high-level steps:

-
- | | |
|---------------|---|
| Step 1 | Upgrade the Cisco CSP 2100 software or perform the initial setup. |
| Step 2 | Log in to the Cisco CSP 2100. |
| Step 3 | Generate and install an SSL certificate. |
| Step 4 | Access the Cisco CSP 2100 through the web interface. |
| Step 5 | Upload the service image to the Cisco CSP 2100. |
| Step 6 | Create a service. |
| Step 7 | Verify the service instance. |
-

Upgrading the Cisco CSP 2100 Software

You can upgrade the Cisco CSP 2100 software from Cisco CSP 2100 Release 2.1.x to Release 2.2.0 by using the Cisco Integrated Management Controller (CIMC) KVM console. Map the ISO image to the Virtual CD/DVD by using the CIMC KVM console and then install the image.

**Note**

You cannot use the following command and REST API to upgrade from Cisco CSP 2100 Release 2.1.x to Release 2.2.0:

- **system install iso update image *imagename***
- **curl -u *username:password* -X POST**
`https://ip-address:port-number/api/running/system/install/iso/update/_operations/update -H "Content-Type: application/vnd.yang.data+json" -d '{"input":{"image":"imagename"}}'`

Performing the Initial Setup

Before You Begin

- Make sure that the Cisco CSP 2100 is set up correctly and is cabled for network access. For information about setting up the Cisco CSP 2100, see the *Cisco Cloud Services Platform 2100 Hardware Installation Guide*.
- Choose a hostname for your Cisco CSP 2100.
- Obtain the following information about the Cisco CSP 2100 from your network administrator:
 - Port channel or physical network interface card (pNIC) to be used as the management interface
 - VLAN values for the management port channel, the management interface, and the dedicated service management interface (optional)
 - Two pNIC members for the port channel to be used as the management interface (optional)
 - Password for the admin user
 - Management IP address
 - Netmask for the management interface
 - Default gateway IP address
 - Domain name server (DNS) (optional)
 - Domain name
 - Port channel or pNIC to be used as the dedicated service management interface (optional)
 - Two pNIC members for the port channel to be used as the dedicated service management interface (optional)

Step 1 Turn on the Cisco CSP 2100.

Step 2 Enter **admin** as the username and **admin** as the password.

Step 3 Enter yes or no depending upon whether you want to use a port channel for the management interface. Configuring a port channel as the management interface ensures that you always have connectivity with the Cisco CSP 2100. You can connect to Cisco CSP 2100 even when one of the pNICs is down. Do one of the following:

- To use a port channel as the management interface, enter **yes** and go to Step 4.
- To use a pNIC as the management interface, enter **no** and go to Step 5.

Step 4 Do the following to use a port channel as the management interface:

- a) Enter a name for the port channel.
- b) Enter the name of the first pNIC.
- c) Enter the name of the second pNIC.
Note Both specified pNICs should be of same speed.
- d) Enter the bond-mode. Valid values are balance-slb, active-backup, and balance-tcp.
- e) Enter the value for the link aggregation control protocol (LACP) for the bond. Valid values are active, passive, and off.
- f) Enter a VLAN value for the port channel. Valid range is from 1 to 4094.

Step 5 Enter the pNIC interface number that you want to use as the management interface. The Linux naming convention designates the four 1-GB Ethernet ports as enp4s0f0, enp4s0f1, enp4s0f2, and enp4s0f3 and the two 10-GB Ethernet ports as enp7s0f0 and enp7s0f1. In addition, there are two 1-GB onboard Ethernet interfaces named enp1s0f0 and enp1s0f1.

Note We recommend that you choose one of the 1-GB Ethernet ports as the management interface, so that you can use the higher bandwidth ports for services.

Step 6 Enter yes or no to specify the shared or dedicated mode for the management interface. Do one of the following:

- To share the management interface with service VMs, enter **yes**. The management interface pNIC carries the management traffic of Cisco CSP 2100 and the management and data traffic of any service using this pNIC.
- To not share the management interface with service VMs, enter **no**. The management interface pNIC carries only the management traffic of Cisco CSP 2100.

Step 7 Enter yes or no depending upon whether you want to specify a VLAN for the management interface. Do one of the following:

- To specify a VLAN for the management interface, enter **yes** and then enter a VLAN value. Valid range is from 1 to 4094.
- To skip specifying a VLAN for the management interface, enter **no**. The VLAN for the management interface is set to 1 by default.

Step 8 Enter **yes** to save the settings.

Step 9 Enter a new password for the **admin** user and then enter the password again for verification.

Step 10 Enter the hostname.

Step 11 Enter the IP address of the management interface.

Step 12 Enter the netmask of the management interface.

Step 13 Enter the IP address of the default gateway.

Step 14 Enter yes or no depending upon whether you want to specify the DNS. Do one of the following:

- To specify a DNS, enter **yes** and enter the IP address of the DNS.

- To skip specifying a DNS, enter **no**.

Step 15 Enter the domain name; for example, cisco.com.

Step 16 Enter **yes** to save the settings.

Step 17 Enter yes or no to configure the dedicated service management interface. Do one of the following:

- To configure a port channel as the dedicated service management interface, enter **yes** and go to Step 18.
- To configure a pNIC as the dedicated service management interface, enter **no** and go to Step 19.

Step 18 Do the following to configure a port channel as the dedicated service management interface:

- Enter a name for the port channel.
- Enter the name of the first pNIC.
- Enter the name of the second pNIC.
Note Both specified pNICs should be of same speed.
- Enter the bond-mode. Valid values are balance-slb, active-backup, and balance-tcp.
- Enter the value for the link aggregation control protocol (LACP) for the bond. Valid values are active, passive, and off.
- Enter a VLAN value for the dedicated service management port channel. Valid range is from 1 to 4094.

Step 19 Enter the pNIC interface number that you want to use as the dedicated service management interface.

Step 20 Enter **yes** to save the settings.

Your specified settings are saved and you are connected to the Cisco CSP 2100 console.

Note The **config terminal** command fails when you run it after performing the initial setup for a new installation. This happens because the admin user is not assigned to a group at the initial login. To run this command and configure Cisco CSP 2100 features, you must log out and then log in to the Cisco CSP 2100.

The following example shows the prompts described in this procedure.

```
localhost login: admin
Password:
```

```
*****
*****
*****
****
**** Cisco Cloud Services Platform 2100 ****
**** Version 2.2.0 ****
**** Built on 2017-02-19 ****
**** Cisco Systems Inc, copyright 2017 ****
****
*****
*****
*****
```

```
Verifying server information ...
```

```
System Information
Manufacturer: Cisco Systems Inc
Product Name: CSP-2100
Version: 2.2.0
```

```

PNIC Remote Connectivity Information from LLDP
=====
PNIC enp1s0f0   : system = No lldp detectd      intf = No lldp detected      state =
down

PNIC enp1s0f1   : system = sw-lab-n5k-3         intf = Ethernet100/1/46      state = up

PNIC enp7s0f0   : system = sw-lab-n5k-3         intf = Ethernet100/1/48      state = up

PNIC enp7s0f1   : system = No lldp detectd      intf = No lldp detected      state =
down

PNIC enp4s0f0   : system = sw-lab-n5k-3         intf = Ethernet100/1/45      state = up

PNIC enp4s0f1   : system = sw-lab-n5k-3         intf = Ethernet100/1/47      state = up

PNIC enp4s0f2   : system = No lldp detectd      intf = No lldp detected      state =
down

PNIC enp4s0f3   : system = No lldp detectd      intf = No lldp detected      state =
down

Enable port channel for mgmt pnic (yes or no): no

Choose a PNIC for the management interface: enp1s0f0, enp1s0f1, enp7s0f0, enp7s0f1, enp4s0f0,
enp4s0f1, enp4s0f2, enp4s0f3:
enp4s0f0
Allow management interface to be shared with service VMs (yes or no)?: yes

Shared Management Interface Physical NIC           : enp4s0f0

Define a vlan for the mgmt interface(yes or no)?: yes
Choose a vlan for the management interface, valid values are between 1 and 4094: 180

Management vlan set to                : 180

Do you want to save these settings (yes or no)?: yes

Please enter a password for the CSP-2100 admin user
The password must:
have at least 8 characters and at most 64 characters
have at least 1 digits
have at least 1 special character[allowed _~#@=+^]
have at least 1 upper case character
have at least 1 lower case character
not have two or more same characters consecutively
not be an exact dictionary word match
Password:
Enter it again for verification:
Password:

Enter your hostname: csp1
Enter your management IP address: 1.2.3.4
Enter your netmask: 255.255.255.0
Enter your default gateway: 1.2.3.1
Do you want to configure a Domain Name Server (DNS) (yes or no)?: yes
Enter your Domain Name Server (DNS): 5.6.7.8
Enter your domain name: cisco.com

System Hostname                : csp1
Management IP Address          : 1.2.3.4
Management Netmask             : 255.255.255.0
Management Gateway             : 1.2.3.1
Domain Name Server (DNS)       : 5.6.7.8
Domain Name                    : cisco.com

Do you want to save these settings (yes or no)?: yes

Saving configuration.....

Do you wish to configure s Dedicated Service Management Port (yes or no)?: yes

```

```

Do you want to set the service mgmt port up as port channel (yes or no)?: yes
Port channel name: SRV-MGMT
Choose the first PNIC for the service mgmt port channel: enpls0f0, enpls0f1, enp7s0f0,
enp7s0f1, enp4s0f0, enp4s0f1, enp4s0f2,
enp4s0f3: enpls0f0

Service Mgmt Pnic member 1 set to          : enpls0f0

Choose the second PNIC for the service mgmt port channel: enpls0f0, enpls0f1, enp7s0f0,
enp7s0f1, enp4s0f0, enp4s0f1, enp4s0f2,
enp4s0f3: enpls0f1

Service Mgmt Pnic member 2 set to          : enpls0f1

Choose bond-mode for service mgmt port-channel(balance-slb or active-backup or balance-tcp)?:
balance-slb
Choose lacp-type for service mgmt port-channel (active or passive or off)?: active
Choose vlan trunk for service mgmt port-channel: 72

Service Mgmt Port Channel: SRV-MGMT
Service Mgmt Member 1      : enpls0f0
Service Mgmt Member 2      : enpls0f1
Service Mgmt Bond Mode     : balance-slb
Service Mgmt LACP type     : active
Service Mgmt VLAN Trunk    : 72

Do you want to save these settings (yes or no)?: yes
CSP-2100 expects HyperThreading to be disabled in BIOS
No Cavium card in the system
No Cavium card in the system
Welcome to the Cisco Cloud Services Platform CLI

TAC support: http://www.cisco.com/tac
Copyright (c) 2015-2016, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

admin connected from 127.0.0.1 using console on csp1
csp1#

```

Logging In to the Cisco CSP 2100

You can log in to the Cisco CSP 2100 by using one of the following modes: web interface (accessible through a web browser), CLI, or REST APIs (accessible through cURL tool or Windows PowerShell). However, before logging in to the web interface or using the REST APIs, you must install an SSL certificate using the CLI. For detailed information about the CLI and available commands, see the *Cisco Cloud Services Platform 2100 Command Reference Guide*.

Generating and Installing an SSL Certificate



Note

For proof-of-concept (POC) or lab deployments, an SSL certificate is not required. You can skip this section and go to [Accessing the Cisco CSP 2100 Web Interface](#), on page 8.

You must generate a Certificate Signing Request (CSR) to send to a Certification Authority (CA) to obtain an SSL certificate and use the CLI to install the SSL certificate on Cisco CSP 2100. The default self-signed certificate installed on the Cisco CSP 2100 is only for temporary use.

Step 1 Log in to the Cisco CSP 2100 CLI in EXEC mode.

Step 2 On the command prompt, use the following command to create a CSR:

```
csp# certificate request sha sha256 keysize 2048
```

After you enter the command, you are prompted for some information such as country name, state, city, email, common name, and so on. For detailed information about this command, see the *Cisco Cloud Services Platform 2100 Command Reference Guide*.

Note The common name is the DNS name of the host, including the domain name; for example, *myserver.mycompany.com*.

Step 3 Provide the required information in the prompt.

After you provide the required information, the following two files are generated in the `/osp/certificates` directory:

- `myhost.csr`—The server certificate request file
- `myPrivate.key`—The server key file

Note To enable the Cisco CSP 2100 to start without entering a password, the `myPrivate.key` file is not protected with a passphrase. However, you can use a passphrase to protect it. When the `myPrivate.key` file is protected with a passphrase, the administrator must enter the password every time the Cisco CSP 2100 starts.

Step 4 Send the `myhost.csr` file to a CA to obtain an SSL certificate.

After you submit the CSR to a CA, the CA generates an SSL certificate and sends a certificate file to you. The CA may also send a certificate chain file.

Step 5 Copy the SSL certificate files that you received from the CA to the `/osp/certificates` directory using the `scp` command from an external server.

Step 6 On the Cisco CSP 2100 command prompt, enter the following command to install the certificate:

```
csp# certificate install-certificate
```

After you enter the command, you are prompted for some information such as localhost (hostname including the domain name), key filename, certificate filename, and chain filename. For detailed information about this command, see the *Cisco Cloud Services Platform 2100 Command Reference Guide*.

Step 7 Provide the required information in the prompt.

After you provide the required information, the SSL certificate is installed.

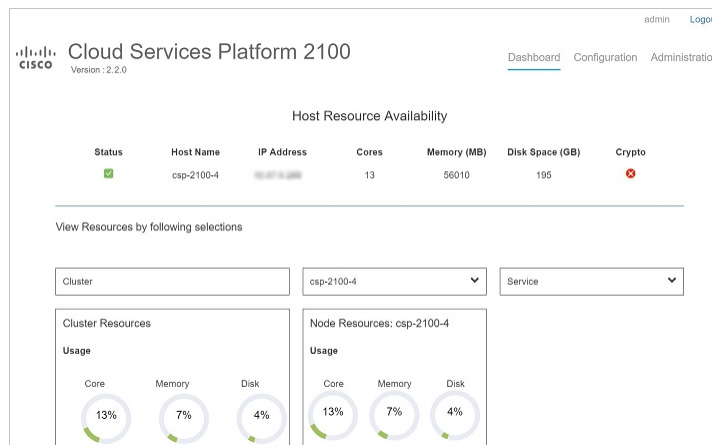
To verify that the certificate is installed, follow the instructions in the next section to log in to the Cisco CSP 2100 web interface using a web browser. After logging in, click the lock icon in the address bar to see information about the installed certificate.

Accessing the Cisco CSP 2100 Web Interface

Step 1 Enter **https://hostname** or **https://ip-address** in a web browser.

Note The hostname should resolve to the IP address that you entered as the management IP address in [Performing the Initial Setup, on page 2](#). The hostname should also match the hostname specified in [Generating and Installing an SSL Certificate, on page 6](#).

Step 2 Enter the username **admin** and the password.
The Cisco CSP 2100 web interface is displayed.



Overview of the Cisco CSP 2100 Web Interface

The Cisco CSP 2100 web interface consists of the following tabs and pages:

- **Dashboard:** The **Dashboard** tab consists of the following pages:
 - **Overview:** Use the **Overview** page to view information about the host resources. You can filter resources by clusters, nodes, and services.
 - **Services View:** Use the **Services View** page to view information about the services traffic rate.
 - **Network View:** Use the **Network View** page to view information about statistics for a pNIC.
- **Configuration:** The **Configuration** page consists of the following pages:
 - **Repository:** Use the **Repository** page to upload or remove an image and to view all available images.
 - **Services:** Use the **Services** page to create a new service or configure existing services, change the power mode of a service, and export a service. You can create a new service using a template or save a service as a template.

- **Service Templates:** Use the **Services Templates** page to view all available service templates and delete a service template.
- **pNICs:** Use the **pNICs** page to view information about pNICs and port channels and to configure or unconfigure a pNIC as the management interface.
- **Port Channel:** Use the **Port Channel** page to create a port channel, delete or edit a port channel, and to configure or unconfigure a port channel as the management interface.
- **SRIOV:** Use the **SRIOV** page to enable, disable, configure, or unconfigure an SR-IOV interface.
- **Administration:** The **Administration** page consists of the following pages:
 - **Password:** Use the **Password** page to change the password for the **admin** user.
 - **Host:** Use the **Host** page to configure the host. You can configure the hostname, host domain name, DNS server, host IP, gateway IP, management MTU, management pNIC mode, and session idle timeout.
 - **NTP Server:** Use the **NTP Server** page to configure an NTP server.
 - **User:** Use the **User** page to create, modify, or delete a local user.
 - **Cluster:** Use the **Cluster** page to create, configure, and delete clusters.
 - **NFS:** Use the **NFS** page to create and configure NFS storage.
 - **SNMP:** Use the **SNMP** page to create and configure SNMP agent, communities, users, groups, and traps.
 - **AAA:** Use the **AAA** page to specify the AAA authentication mode and to create, modify, or delete a TACACS+ or RADIUS server.
 - **IP Receive ACL:** Use the **IP Receive ACL** page to configure the Access Control List (ACL) access for the management interface. You can specify the source network IP address, service type, priority, and action for the packets received from the specified source network.

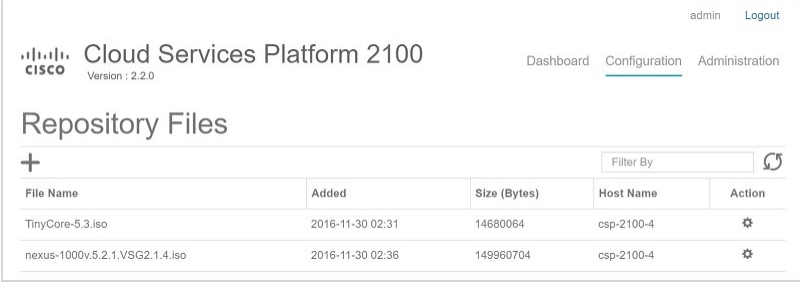
Uploading Service Images Using the Cisco CSP 2100 Web Interface

Before You Begin

Be sure to download the service image to your local machine or a location on your local network that is accessible to your Cisco CSP 2100.

-
- | | |
|---------------|--|
| Step 1 | Click the Configuration tab and then choose Repository . |
| Step 2 | On the Repository Files page, click the add button (+). |
| Step 3 | Click Browse . |
| Step 4 | Navigate to the service image, select a service image, and click Open . |
| Step 5 | Click Upload .
After the service image is uploaded, the image name and other relevant information are displayed in the Repository Files table. |

Tip You can also use this procedure to upload the banner files and the configuration files to the repository.



The screenshot shows the Cisco Cloud Services Platform 2100 web interface. At the top, there's a header with the Cisco logo, the title 'Cloud Services Platform 2100', and the version 'Version : 2.2.0'. On the right, there are links for 'admin' and 'Logout'. Below the header, there are three tabs: 'Dashboard', 'Configuration' (which is selected), and 'Administration'. The main content area is titled 'Repository Files'. It features a '+' button to add new files, a 'Filter By' search box, and a refresh icon. Below this is a table listing repository files.

File Name	Added	Size (Bytes)	Host Name	Action
TinyCore-5.3.iso	2016-11-30 02:31	14680064	csp-2100-4	
nexus-1000v.5.2.1.VSG2.1.4.iso	2016-11-30 02:36	149960704	csp-2100-4	

Creating a Service Instance

Step 1 Click the **Configuration** tab and then choose **Services**.

Step 2 On the **Service** page, click the add (+) button.
The **Create Service** page is displayed.

Cloud Services Platform 2100
Version : 2.2.0

Dashboard Configuration Administration

Service

Create Service

* Required Field

☒ Create Service ☐ Create Service using Template

Name: *

Target Host Name: *

VNF Management IP:

Image Name: *

Number of Cores:
Available Cores: 13

Disk Space (GB):
Available Disk Space (GB): 195

RAM (MB):
Available RAM (MB): 56010

☐ NFS Storage

Disk Type: ☒ IDE ☐ VIRTIO

VNIC *

Storage

VNC Port:

VNC Password:

Confirm VNC Password:

Serial Port

☐ HA Service Configuration

Step 3 In the **Name** field, enter a name for the service.

Step 4 From the **Target Host Name** drop-down list, choose the target host.

Step 5 (Optional) In the **VNF Management IP** field, enter the VNF management IP address to be used in the service.

Note The VNF Management IP value entered in this field does not get configured in the service. This field serves only as a reference to the VNF management IP address mapped to a service.

Step 6 From the **Image Name** drop-down list, choose an image file for the service.

You can use an ISO or OVA, or a QCOW software image file to create the service.

Note With Cisco VSM and Cisco VSG services, only ISO image files are supported.

Depending on the type of image selected, additional fields are displayed. If your service requires additional information, as is the case with Cisco VSM and Cisco VSG services, you must enter this information in the **Additional Image Questionnaires** section. For details about the additional information that your service requires, see the documentation for that service.

- Step 7** (Optional) In the **Number of Cores** field, specify the number of cores. Make sure that the new value does not exceed the available resources.
- Step 8** (Optional) In the **Disk Space (GB)** field, specify the hard disk space. Make sure that the new value does not exceed the available resources.
- Step 9** (Optional) In the **RAM (MB)** field, specify the RAM. Make sure that the new value does not exceed the available resources.
- Step 10** (Optional) If you want to deploy the service on an NFS storage, select the **NFS Storage** check box and then select an NFS storage from the **NFS** drop-down list.
- Step 11** (Optional) In the **Disk Type** field, specify the disk type. Valid choices are IDE or VIRTIO.
- Step 12** Click **VNIC** and in the **VNIC Configuration** dialog box, do the following:
- a) In the **Interface Type** field, specify the type. Valid choices are Access, Trunk, and Passthrough. Depending on the selected interface type, the fields of **VNIC Configuration** dialog box are displayed. The following table describes these fields based on the interface type.

Field	Interface Type	Description
VLAN	<ul style="list-style-type: none"> • Access • Trunk • Passthrough (only for SR-IOV and MACVTAP passthrough modes) 	In the VLAN field, enter the VLAN ID. Valid range is from 1 to 1000 and from 1025 to 4094.
Native VLAN	Trunk	In the Native VLAN field, specify the VLAN ID. Valid range is from 1 to 1000 and from 1025 to 4094.
Model	<ul style="list-style-type: none"> • Access • Trunk • Passthrough (only for MACVTAP passthrough modes) 	In the Model field, specify the model number of the vNIC driver. Valid choices are Virtio (for the KVM driver) and e1000 (for the Intel Ethernet driver).

Field	Interface Type	Description
Service Management Interface	<ul style="list-style-type: none"> • Access • Trunk • Passthrough 	<p>If you want to use the dedicated service management interface with this service, select the Service Management Interface check box.</p> <p>Note This check box is displayed only if a pNIC or a port channel has already been configured as the dedicated service management interface. When you select this check box, the Network Name field is automatically populated with the name of the configured dedicated service management interface and you do not need to specify the network name.</p>
Network Type	<ul style="list-style-type: none"> • Access • Trunk 	<p>In the Network Type field, specify the network type. Valid choices are Internal and External.</p> <p>Create an internal network when you need to connect one service to another service and there is no connection to a physical network interface card (pNIC). Create an external network when you want to connect to a pNIC directly (passthrough) or through a switch.</p>
Network Name	<ul style="list-style-type: none"> • Access • Trunk • Passthrough 	<p>In the Network Name field, specify the name of the network.</p> <p>To create an internal network, enter a name for the internal network in the Network Name field. To create an external network or to specify the network name for the passthrough mode, choose a network interface from the Network Name drop-down list.</p>
Passthrough Mode	Passthrough	<p>In the Passthrough Mode field, specify the passthrough mode. Valid choices are SR-IOV, PCIE, and MACVTAP.</p>

b) When you are satisfied with the vNIC configuration, click **Submit**.

To add more vNICs, click **VNIC** and repeat all tasks described in this step.

Step 13 (Optional) Click **Storage** and in the **Storage Configuration** dialog box, do the following:

a) In the **Type** field, specify the storage type. Valid choices are Disk and CDROM.

Depending on the selected storage type, the fields of **Storage Configuration** dialog box are displayed. The following table describes these fields based on the storage type.

Storage Type	Field	Description
Disk	Location	In the Location field, select a location. You can select a local or remote location. A remote location is displayed only if you have already configured an NFS storage.
Disk	Disk Type	In the Disk Type field, specify the disk type. Valid choices are IDE and VIRTIO.
Disk	Format	In the Format field, specify the disk format. Valid choices are RAW and QCOW2.
Disk, CDROM	Size (GB)	In the Size (GB) field, enter the disk size.

b) When you are satisfied with the storage configuration, click **Submit**.

To add more storage, click **Storage** and repeat all tasks described this step.

Step 14 (Optional) In the **VNC Port** field, enter a VNC port for the service. Valid range is from 8721 to 8784.

Step 15 (Optional) In the **VNC Password** field, enter a password and then enter the same password in the **Confirm VNC Password** field.

Caution We strongly advise that you secure your remote access with a complex alphanumeric password for VNC.

Note The VNC console password is in clear text which might be indicated as a security issue. To ensure that the VNC console access is secure in Cisco CSP 2100, the VNC console is accessible only through the web interface which is protected by a user name and a password.

Step 16 Click **Serial Port** and in the **Serial Port** dialog box, do the following:

- In the **Type** field, specify the port type. Valid choices are **Telnet** and **Console**.
 - If you have selected Telnet type in Step a, then in the **Service Port Number** field, enter a value. Valid range is from 7000 to 8700.
 - When you are satisfied with the serial port configuration, click **Submit**.
- To add more serial ports, click **Serial Port** and repeat all tasks described in this step.

Step 17 (Optional) If you are configuring the services in redundancy, select the **HA Service Configuration** check box. The Cisco CSP 2100s must be in the cluster mode. Do the following:

- In the **Name** field, enter the name of the secondary service.
 - From the **HA Host Name** drop-down list, choose a Cisco CSP 2100 remote peer that is a part of the cluster.
 - In the **VNF Management IP** field, enter the VNF management IP address for the secondary service.
 - In the **VNC Port** field, enter a VNC port for the secondary service. Valid range is from 8721 to 8784.
 - Click **Secondary VNIC** to add a secondary VNIC.
- The VNIC Configuration dialog box is displayed. For information about the fields of this dialog box, see Step 12.
- All other parameters that need to be configured in the secondary service are inherited from the already-configured primary service.

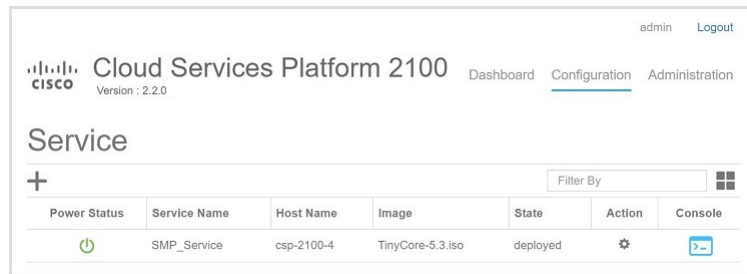
Step 18 Click **Deploy**.
The Service Test Creation dialog box is displayed indicating that the service is available.

Verifying Your Service Instance




Make sure that your service instance is up and running.

Step 1 Click the **Configuration** tab and then choose **Services**.
The **Service** table shows the current status of services.

Step 2 Find your service instance in the **Service Name** column, and check that the state is deployed and the power status is on.



The screenshot shows the Cisco Cloud Services Platform 2100 Configuration page. The top navigation bar includes 'admin' and 'Logout'. The main header shows 'Cloud Services Platform 2100' with 'Version : 2.2.0' and tabs for 'Dashboard', 'Configuration', and 'Administration'. The 'Configuration' tab is active. Below the header, the 'Service' section is displayed with a '+ Add' button and a 'Filter By' dropdown. A table lists the service instances:

Power Status	Service Name	Host Name	Image	State	Action	Console
	SMP_Service	csp-2100-4	TinyCore-5.3.iso	deployed		

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.